Published and Copyright (c) 1999 - 2011
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe,
log on to our website at: www.atarinews.org
and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org
and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to
subscribe from.

To download A-ONE, set your browser bookmarks to one of the
following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1320 05/20/11

~ Firefox 4 Ahead of IE9! ~ People Are Talking! ~ Privacy by Default!
~ Eee Pad Tablet to Laptop ~ Safety on Macs Waning! ~ Update to the ECPA?
~ New Virus Attacks Macs ~ More Problems for PSN! ~ No Appeal for Twins!

~ Desktop Linux Growing! ~ The End of Snow Days?! ~ Post-PC Era Is Here!

-* U.S. Values for the Internet *-
-* Death Penalty for Web Sites Backed! *-
-* RIM Recalls 1,000 PlayBook Tablet Computers *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
"""""""""""""""""""""""""""""

Well, it looks like there really is a large star in the sky - that yellow orb that we haven't seen in a few weeks here! Cold and wet days just don't do much for one's well-being as far as I'm concerned. But, there is a chance that we'll catch more than a glimpse of the sun over the next few days! It's about time, Memorial Day weekend is just around the corner!

Until next time...

=~=~=~=

->In This Week's Gaming Section - Duke Nukem Forever Demo in June!!
""""""""""""""""""""""""""""""""" Sony Begins Restoring PSN!
PSN Security Flaw, and Hacked Again!

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!
""""""""""""""""""""""""""""""""""""""

'Duke Nukem Forever' Demo Launching June 3 (Yes, For Real)

Duke Nukem Forever, six-time winner of Wired magazine's "Vaporware Award," is on track to hit stores in the U.S. on June 14 and internationally on June 19.

"That is the REAL date. This one is FOR REAL," proclaimed Andy Pitchford, president of Gearbox Software, the publisher of DNF, in a "special message" on Tuesday (see video below). "It's going to happen!"

Pitchford also announced a demo video arriving on June 3, but only to members of the First Access Club, which requires pre-ordering the game

at official U.S. retailers GameStop or Amazon.

Both retailers offer the game for $59.99 for the Xbox 360 or PlayStation 3 and $49.99 for the PC version. GameStop's pre-order package includes an in-game EGO boost, Big Head mode, and T-shirt pack. Amazon's offer includes three free MP3 music downloads.

A list of official retailers in your country is available on dukenukemforever.com.

If you're not enthused about the preview demo, you can also pre-order the game for slightly less at Wal-Mart or Direct2Drive.

First announced in 1997 and slated for release in 1998, DNF is the most delayed title in modern gaming history. At last count, the game was due to come out on May 3, but was inexplicably delayed six weeks ago via a "special message" on March 24.

Despite the endless teasing, legions of Duke fans have held on to the hope that the game would come out any day now. Like PCMag analyst Matthew Murray, who tested the game in February and was promised by Pitchford himself that the game would come out on May 3.

Sony Begins Restoring PlayStation After Security Breach

Sony said it had begun restoration of its PlayStation Network games service on Sunday, almost a month after a massive security breach of the network forced the company to shut it down.

Gamers and security experts had criticized Sony for its handling of the incident, which sparked lawsuits and cast a shadow over its plans to combine the strengths of its content and hardware products via online services.

The Japanese electronics and entertainment giant apologized to customers for the outage, and said a range of new security measures had been introduced. These included an early warning system that could alert the company to any attempt to penetrate the network.

"I can't thank you enough for your patience and support during this time," Sony No. 2 Kazuo Hirai said in the news release, which was also posted as a video message on the PlayStation Network blog.

"We are taking aggressive action at all levels to address the concerns that were raised by this incident, and are making consumer data protection a full-time, companywide commitment."

A single message from a PlayStation Network user under the name SG-1_F-302 on the blog read simply: "Thank you Sony!!!!"

But some users have said the prolonged outage has prompted them to switch to rival Microsoft's Xbox Live games service.

In what is thought to be the biggest security breach of its kind, hackers accessed personal information on 77 million PlayStation Network and Qriocity accounts, 90 percent of which are in North America and Europe, and may have stolen credit card information.

Hackers rented a server from Amazon for the attack, Bloomberg news said earlier in the day, citing a source with knowledge of the matter.

Sony discovered unusual activity on its PlayStation Network, which enables games console owners to download games, chat with friends and pit their skills against rivals, on April 19.

It shut down the network and its Qriocity online music and movie service, frustrating many users, but waited almost a week before alerting users to the extent of the security leak.

The company later found out that a separate online games service had also been penetrated, allowing access to another 25 million user accounts.

Sony said the restoration of PlayStation Network and Qriocity online movie and music services would take place on a country by country basis and that it expected the process to be complete by May 31.

Sony Online Entertainment services are also being restored and customers will be offered free game time as compensation for the outage, the company said.

Sony also said it had appointed an acting chief information officer to oversee security on its networks.

The attack on Sony is the highest-profile of a series that have affected large corporations in recent months, fuelling doubts about the security of cloud computing services.

"During the past 18 months, we've seen a dramatic rise in the volume of cyber attacks, their sophistication and their impact on businesses," Sony quoted Francis deSouza of Internet security company Symantec as saying.

Japanese games company Square Enix, known for the Final Fantasy series, said on Saturday that hackers had accessed one of its websites and obtained information, including up to 25,000 customer e-mail addresses and possibly job applicants' resumes.

Sony Finds Another Security Flaw, Shutters Site

Sony Corp has shut down a website set up to help millions of users affected by April's massive data breach after finding a "security hole".

The site had been designed to help 77 million users of its PlayStation Network reset their passwords after finding the security weakness.

The issue, which Sony alerted customers to on its PlayStation website, marks yet another setback for the company, which has been under fire since hackers broke into its systems about a month ago.

Sony spokesman Dan Race said the company found the security hole on a webpage that could potentially allow the hackers who had breached personal data from users in April to access their accounts using the data they had stolen.

"If I had your email and your birth date I could have potentially got access to your account," Race said.

In response, Sony on Wednesday temporarily took down the PlayStation Network password reset page, as well as that of its Qriocity music service. It has since fixed the issue and will bring the pages back up shortly, Race added.

Sony last month disclosed that it had been a victim in one of the biggest cyber-attacks in history.

It shut down its PlayStation Network across the globe in mid-April and has slowly started to restore access, starting in the United States. The company is still working with Japanese government authorities to restore access in that country.

Analysts said the company faces a tough road ahead in addressing the security issues brought to light by the scandal.

"This is one of the things that was probably overlooked and forgotten by Sony," said Maxim Group analyst Mark Harding.

John Bumgarner, a well-regarded Internet security researcher and U.S. military special operations veteran, last week told Reuters he had identified a handful of flaws that would be easy for a hacker to identify and potentially exploit.

He said on Wednesday that he wasn’t surprised by Sony’s latest gaffe because security flaws remain across the company’s vast computer networks.

"The Sony network in general still isn’t secure and still has security issues that could be exploited by hackers," said Bumgarner, who is chief technology officer for the U.S. Cyber Consequences Unit, a nonprofit group that monitors Web threats.

Sony said no hacking had taken place on this website and that PlayStation Network account holders can still change their passwords on their PlayStation consoles at home.

On Tuesday, Chief Executive Howard Stringer fired back at critics for saying Sony had not acted quickly enough to inform consumers about April’s data breach.

The notice to users about the website shutdown can be found here: http://bit.ly/JkCma

Hackers Hit Sony Sites Raising More Security Issues

Sony Corp has been hacked again, exposing more security issues for the company less than a month after intruders stole personal information from more than 100 million online user accounts.

A hacked page on a Sony website in Thailand directed users to a fake site posing as an Italian credit card company. The site was designed to steal information from customers, Internet security firm F-Secure disclosed on Friday.

It is the latest in a series of security headaches for Sony, which discovered in April hackers had broken into its PlayStation Network and stole data from more than 77 million accounts. On May 2, Sony disclosed hackers had also stolen data from about 25 million user accounts of the Sony Online Entertainment website, a PC-based games service.

The PlayStation attack, considered the biggest in Internet history, prompted the Japanese electronics giant to shut down its PlayStation Network and other services for close to a month.

"It’s a Sony security issue," said Jennifer Kutz, a representative for F-Secure, referring to the fraudulent website.

The latest hacking, which the security company said occurred separately from the April attack, was reported just hours after Sony told customers of another breach on one of its units.

So-Net, the Internet service provider unit of Sony, alerted customers on Thursday that an intruder had broken into its system and stolen virtual points worth $1,225 from account holders.

Critics have slammed the company for not protecting its networks securely and then waiting up to a week before telling its customers of the attack and the possible theft of credit card information, prompting lawmakers and state attorneys general to launch investigations.

Security experts said they were not surprised that the electronics company has not yet fixed weaknesses in its massive global network. Earlier this week, Sony shut down one of its websites set up to help millions of users change their passwords after finding a security flaw.

"Sony is going through a pretty rigorous process and finding the holes to fill," said Josh Shaul, chief technology officer for computer security firm Application Security Inc.

"The hackers are going through the same process and they’re putting their fingers in the holes faster than Sony can fill them."

"What we’ve done is stopped the So-Net points exchanges and told customers to change their passwords," So-Net said in a statement in Japanese to consumers.

About 100,000 yen ($1,225) was stolen from accounts that were attacked. The company said there was no evidence other accounts in the online system had been compromised.

"At this point in our investigations, we have not confirmed any data leakage. We have not found any sign of a possibility that a third party has obtained members’ names, address, birth dates and phone numbers."

Security experts have told Reuters Sony’s networks around the world remain vulnerable to attack.

Sony’s string of security problems could be attracting more hackers to attack its networks.

"I think it’s now ’I’m a hacker and I’m bored, let’s go after Sony,’" Shaul said.

A Sony representative in the United States could not immediately be

reached for comment on Friday.

=~=~=~=

A-ONE's Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

Privacy By Default: California Social Networking Bill Makes Sense

Facebook, Google, Skype, and Twitter have joined forces to oppose a bill from a California senator that would force online services to lock down personal information by default. The united front from the Internet, though, illustrates exactly why such a bill might just be the solution we need.

California Senator Ellen Corbett, D-San Leandro, introduced SB 242 which would force online services and social networking sites to make default settings private (except for the user's name and city of residence), and force users to choose their privacy settings when they register.

The giants of the Internet have allied to fight against the bill. In a letter to Corbett, the group asserts that this legislation would undermine the ability of Californians to make informed, meaningful choices about the use of their personal data.

I'm sorry, what? How is taking a model that assumes nothing is private, and changing it to a system where privacy is granted by default, but users must make informed, meaningful choices to allow their information to be shared going to undermine that ability exactly?

What is wrong with locked down by default? The Constitutional right to free speech is not violated, because the option to open the floodgates and share your personal information with the world would still be there. But, it would give users better control over their own information, and it would mean that the decision to share personal data would be a conscious one.

It doesn't make any sense to argue that open by default with the option to impose privacy restrictions is reasonable, but that locked down by default with the option to remove privacy restrictions is a heinous violation of personal liberty.

Either way, there is an assumed obligation of the user to understand the risks and implications of their privacy choices, and to either impose or remove privacy controls to meet their needs. But, many users are not aware of the privacy implications, and never take the time to learn about the privacy options available. Flipping the model around would force users to make conscious choices about privacy in order to effectively use the sites and services.

What seems more likely is that Facebook, Google, and others are afraid of what locked down by default might do to their business model and the

ability to farm and exploit useful information from those unlocked user profiles. But, if users really want to share their information as Zuckerberg has asserted on multiple occasions - and that does seem like a reasonable assumption for a social networking site - then they will make the choice to remove the privacy restrictions and all will be back to normal.

Bill Would Require Warrants For Govt. to Access Your Email, Cloud Services

Sen. Patrick Leahy on Tuesday unveiled an overhaul to a 25-year-old digital privacy law that would require the government to obtain warrants before accesssing email and other cloud-based data.

The update to the Electronic Communications Privacy Act (ECPA), would also extend to location-based data, and allow private companies to collaborate with the government in the event of a cyber attack.

The ECPA was first enacted in 1986, well before the Internet, email, or smartphones. As a result, it is "significantly outdated and out-paced by rapid changes in technology and the changing mission of our law enforcement agencies after September 11," said Leahy, a Vermont Democrat.

As a result, Leahy’s updated 2011 version of the ECPA would apply to technologies like email, cloud services, and location data on smartphones. If the government wanted an ISP to hand over emails on a particular customer, for example, they would need to first obtain a warrant. At this point, the government abides by a rule that provides access to email after 180 days, depending on the circumstance.

"The bill gets rid of the so-called ’180-day rule’ and replaces this confusing mosaic with one clear legal standard for the protection of the content of emails and other electronic communications," Leahy said in a statement.

If the government obtains access, they would have to notify the person involved and provide them with a copy of the warrant within three days. If it’s a sensitive investigation, and the government doesn’t want to tip off the alleged offenders right away, it can delay notification by up to 90 days via court order, which can be extended another 90 days, if necessary. There can also be a delay for national security reasons.

In the wake of a controversy over how smartphones collect user data, the updated ECPA would also require warrants or a court order under the Foreign Intelligence Surveillance Act for location-based data.

"There are well-balanced exceptions to the warrant requirement if the government needs to obtain location information to address an immediate threat to safety or national security, or when there is user consent or a call for emergency services," Leahy said.

A warrant for location information must still be obtained within 48 hours, even in an emergency, or a court might suppress the data gathered. There is also an exception when a user provides consent or calls for emergency services.

The government could use an administrative or grand jury subpoena in order to get certain info from an ISP, including: customer name,

address, session time records, length of service information, subscriber number and temporarily assigned network address, and means and source of payment information.

Taking a page from the cyber-security plan unveiled by the Obama administration last week, Leahy's plan also allows for collaboration between the government and private companies if those companies are the victim of a cyber attack.

"The legislation creates a new limited exception to the nondisclosure requirements under the ECPA, so that a service provider can voluntarily disclose content to the government that is pertinent to addressing a cyberattack," Leahy said. "To protect privacy and civil liberties, the bill also requires that, among other things, the Attorney General and the Secretary of Homeland Security submit an annual report to Congress detailing the number of accounts from which their departments received voluntary disclosures under this new cybersecurity exception."

The bill comes several days after Leahy introduced the PROTECT IP Act, which would allow the U.S. government to go after "rogue Web sites" that contain infringing content.

U.S. Lays Out Priorities for Future of Cyberspace

The United States launched a new initiative Monday designed to stamp the Internet with U.S. values such as freedom of expression, saying cyberspace must remain open, secure and reliable.

U.S. Secretary of State Hillary Clinton and a host of other senior government officials unveiled a new national strategy on cyberspace that seeks to enshrine open international standards for the Internet while protecting network security and strengthening law enforcement.

"There is no one-size-fits-all, straightforward route to this goal. We have to build a global consensus about a shared vision for cyberspace," Clinton said.

The new strategy codifies the Obama administration's aggressive attempts to define the future of the Internet in the face of competing models such as that promoted by China, which practices greater control.

Clinton, who has repeatedly underscored the centrality of Internet freedom to U.S. foreign policy, said the goal was an open global system that both fosters innovation and economic growth while strengthening security and free expression.

"While the Internet offers new ways for people to exercise their political rights, it also, as we have seen very clearly in the last months, gives governments new tools for clamping down on dissent," Clinton said.

The U.S. approach has put it on a collision course not only with Beijing but also with authoritarian governments elsewhere - particularly in the Middle East, where some governments have sought to use Internet controls to block expressions of political unrest sweeping the region.

The United States funds programs to both develop new technologies and

train activists to evade government controls. But activists accuse the U.S. government of hypocrisy for insisting the Internet must also have "rule of law" - a signal that unauthorized information breaches such as the WikiLeaks dump of classified State Department cables will not be tolerated.

Commerce Secretary Gary Locke, nominated as the next U.S. ambassador to China, said he intended to keep pressing "to advance these goals and the broader set of cyberspace issues with our Chinese counterparts."

The new U.S. strategy contains few specifics but outlines priorities which include building Internet capacity, improving Internet governance and promoting military cooperation on cyberspace issues to protect networks from attack.

The U.S. military's new Cyber Command became fully operational last year and is working to prevent break-in attempts by more than 100 foreign intelligence organizations seeking to hack into some of the 15,000 U.S. military computer networks, U.S. officials say.

The Obama administration is also pressing Congress to pass strong cybersecurity measures to protect consumers' personal information and safeguard the U.S. financial system and electric power grid from potentially devastating attacks.

Several cybersecurity bills have limped along in Congress over the past year despite high-profile hacker attacks on Nasdaq OMX Group and Sony Corp. Some companies resist what they say is regulatory overreach by the government.

Senate Bill Amounts to Death Penalty for Web Sites

A new bill backed by movie studios and other large copyright holders takes a novel approach to curbing access to piratical Web sites: an Internet death penalty.

That's a good way to describe the approach adopted by the legislation introduced today, which specifies a step-by-step method for making Web sites suspected of infringing copyrights or trademarks vanish from the Internet. It's called the Protect IP Act.

The U.S. Department of Justice would receive the power to seek a court order against an allegedly infringing Web site, and then serve that order on search engines, certain Domain Name System providers, and Internet advertising firms - which would in turn be required to "expeditiously" make the target Web site invisible.

It's not entirely clear how broad the Protect IP Act's authority would be. An earlier draft (PDF) of the legislation would have allowed the Justice Department to order any "interactive computer service" - a phrase courts have interpreted to mean any Web site - to block access to the suspected pirate site.

But the final version (PDF) refers instead to "information location tool." That's defined as a "directory, index, reference, pointer, or hypertext link," which would certainly sweep in Google, Yahoo, and search engines, and may also cover many other Web sites.

This is the main process through which the Internet death penalty is imposed. The Protect IP Act says that an "information location tool shall take technically feasible and reasonable measures, as expeditiously as possible, to remove or disable access to the Internet site associated with the domain name set forth in the order." In addition, it must delete all hyperlinks to the offending "Internet site."

In other words, the targeted Web site would start to vanish from the Internet in the United States.

Any copyright holder also could file a lawsuit and seek to levy a less dramatic form of Internet punishment, blocking only "financial transactions" and "Internet advertising services" from doing business with the suspected infringer.

Sponsors of the Protect IP Act include Judiciary Committee Chairman Patrick Leahy (D-Vt.), as well as Orrin Hatch (R-Utah), Chuck Grassley (R-Iowa), Charles Schumer (D-N.Y.), Dianne Feinstein (D-Calif.), Sheldon Whitehouse (D-R.I.), Lindsey Graham (R-S.C.), Herb Kohl (D-Wis.), Chris Coons (D-Del.), and Richard Blumenthal (D-Conn.).

Leahy said in a statement that his proposal permits law enforcement to "crack down on rogue Web sites dedicated to the sale of infringing or counterfeit goods." The actual bill text, however, doesn't require that the piratical Web site sell anything - meaning, for example, if WikiLeaks were accused of primarily distributing copyrighted internal bank documents, access from the United States could be curbed.

The Protect IP Act doesn't appear to require broadband providers (which probably aren't "information location tools") to block the Internet address of the targeted Web site. Which may be why the National Cable and Telecommunications Association applauded the measure in a statement saying its introduction will address "the growing issues of online piracy and illegal content distribution that are hurting America's content industry and consumers."

"We want to thank Chairman Leahy, Senator Hatch, and the other co-sponsors for recognizing the true cost of online content theft and for seeking new tools to effectively enforce U.S. laws on the online marketplace," said Michael O'Leary, executive vice president of the Motion Picture Association of America (PDF). And the U.S. Chamber of Commerce was no less enthusiastic, calling the bill an "enhanced legal tool against 'rogue sites,' which steal American jobs and threaten consumers' health and safety."

Sherwin Siy, deputy legal director at Public Knowledge, said: "I can appreciate that the drafters are trying to address some of the overbreadth issues, but I think that the core of the bill remains a problem." And the Computer and Communications Industry Association, which represents some Internet companies, called Protect IP an "Internet censorship bill" under a "new name."

The Protect IP Act is a successor to last fall's bill known as COICA, for Combating Online Infringement and Counterfeits Act. That bill used different procedures, but also allowed the government to pull the plug on Web sites accused of aiding piracy.

Another bill introduced Thursday would make the illegal streaming of copyrighted works a federal felony, a proposal that follows a White House recommendation in March.

RIM Recalls 1,000 PlayBook Tablet Computers

BlackBerry smartphone maker Research In Motion Ltd. has recalled about 1,000 of its BlackBerry PlayBook tablet computers due to defective operating software that can make it impossible for users to set up the device.

The Waterloo, Ontario-based gadget maker said in a statement Monday that it learned that the affected tablets were shipped with software "that may result in the devices unable to properly load software upon initial set-up." Only PlayBooks with 16 gigabytes of memory were affected, RIM said, and the majority of them had not yet been sold to customers.

RIM said it is working to replace the affected tablets. Customers that did end up with one that can't load the software correctly during setup can contact the company for help, RIM said.

The issue was reported on Saturday by tech blog Engadget, which said the affected PlayBooks had been shipped to Staples Inc. stores. Staples spokeswoman Carrie McElwee confirmed that the devices had been sent to the company's stores.

The PlayBook - which costs $499-$699, depending on the amount of built-in storage space - received mixed reviews when it was released in April. The device marks RIM's first effort to branch out from its smartphone base and capture a portion of the tablet computer market. Apple Inc. popularized the tablet when it released its first iPad last year, and the device - which was recently upgraded - has dominated that market ever since.

The recall is RIM's most recent bit of bad news. The gadget maker slashed its fiscal first-quarter forecast last month, saying it is selling fewer and cheaper smartphones than it anticipated. The company's previous prediction for the quarter had already been below analyst expectations.

Though RIM's BlackBerry smartphones are known for their security and reliability as email devices, they haven't kept up with iPhones or phones that use Google Inc.'s Android software when it comes to running third-party applications.

Eee Pad Tablet Transforms into Laptop

The tablet computers that compete with the iPad have mostly been uninspiring. The Eee Pad Transformer stands out with a design that isn't just copied from the iPad: It's a tablet that turns into a laptop.

For $399, $100 less than the cheapest iPad, you get a tablet computer with a 10-inch screen and hardware that doesn't cut corners. It's fully usable on its own. For another $149, you can buy a keyboard that connects to the tablet. Together, they look and open like a small laptop.

The Transformer is made by Asustek Computer Inc., the Taiwanese company

that started the brief "netbook" craze a few years ago by selling small, inexpensive laptops. With the keyboard attached, the Transformer is nearly indistinguishable from a netbook.

But before you get too excited about the prospect of a laptop-tablet hybrid that combines the best of both worlds, I have to tell you that you're not getting a Windows laptop in the bargain. The Transformer runs Google Inc.'s Android software, originally designed for smartphones.

That means it doesn't run full-blown Windows programs or connect to peripherals such as scanners. This isn't all a bad thing, as Android comes with important advantages, such as a long battery life, programs designed for touch input and a computer that comes to life almost immediately when you open the lid.

The keyboard may sound a bit expensive for $149, but it does more than help with typing. It has a track pad with "mouse buttons," just as you'd find on a laptop. It also contains an extra battery that charges the tablet's battery, two USB ports for connecting peripherals and a slot for SD memory cards, used in most digital cameras.

I tested the battery life by playing a high-definition video over and over again, with the screen set to medium brightness. I got a respectable nine hours from the tablet alone and 13 hours with the keyboard attached. That compares with 10 hours for the iPad 2.

The screen uses the same technology as the iPad's, making it easy to read from any angle and in any orientation. It is slightly larger than the iPad's and has a slightly higher resolution.

The Transformer has two cameras, as we expect from this year's tablets. The picture quality is so-so but more than adequate for videoconferencing through Google Talk.

Of course, you could get an iPad and an accessory keyboard instead. There are good reasons for doing so - I'll talk more about the software below - but let's stick for the moment to discussing what's good about the Transformer.

The iPad doesn't make any particular accommodation for a keyboard. The accessory ones connect using short-range Bluetooth wireless technology, which can be a hassle to connect and troubleshoot. It also means the keyboards need separate batteries - Apple's own model uses two AAs. The battery in the Asus keyboard doesn't need to be charged for the keyboard to work, and in any case, it uses the same charger as the tablet.

Most iPad keyboards don't attach to the tablet itself, because there's nothing to hang on to. This is fine if you're at a table, but juggling an iPad and a separate keyboard on your lap can be difficult. Some iPad keyboards are built into a case, which covers the tablet and forms a laptop-like unit, though an inelegant one.

The Transformer has two slots for the keyboard to lock into, forming a sturdy whole that's easy to use on a lap or tummy, for those really lazy moments on the couch.

There's another nice thing about the Transformer keyboard: The keys are designed for the software. There are keys that bring you to the Home screen and Settings. Others control screen brightness, volume and media playback. There are buttons for the Back and Menu functions of Google's

Android software.

This isn’t the first time we’ve seen small laptops running Android, but it is the first time I’ve used one that runs Honeycomb, the first Android version specifically designed for tablets rather than smartphones. The update makes Android much better at taking advantage of a 10-inch screen.

But as tablet software, Android is still far behind Apple’s iOS software for the iPad. The biggest problem is the low quality and poor selection of applications from outside companies. Many of my favorite iPad apps, including Netflix and The Wall Street Journal are not available at all. Others, such as The New York Times, are available only in inferior versions, designed for the smartphone screen rather than the tablet.

I also had frequent crashes when using the applications. The Transformer is perhaps the best Android tablet out there, especially considering the price, but the software is still a major weakness. Still, the beautifully integrated keyboard should tempt people who don’t want to decide between a tablet and a laptop.

Firefox 4 Races Further Ahead of IE9

Mozilla may still be weeks away from automatically upgrading users of its aging Firefox 3.5 browser, but even without the benefit of those additional users its latest browser version continues to blast past Microsoft’s competing Internet Explorer 9 in usage.

In fact, early this month Firefox 4’s usage began to show a sharp increase while IE9 continued on a much more gradual climb, Mozilla’s Asa Dotzler pointed out on Sunday.

"Since activating the Firefox Update system and alerting Firefox 3.5 and 3.6 users to the availability of Firefox 4, the line has really picked up some speed," Dotzler wrote in a blog post with an accompanying graph.

"Internet Explorer 9’s trajectory looks very similar to what we saw with IE8 and IE7 before it," he added. "Microsoft pushes new versions at an excruciatingly slow pace."

According to the StatCounter data Dotzler based his analysis on, Firefox 4 accounted for close to 16 percent of the browser market on Monday, he said, while IE9 was approaching 5 percent. "IE9’s steady progress should put it around 10 percent in a couple of months," he predicted.

Mozilla recently announced that in June it will begin automatically upgrading users of its Firefox 3.5 browser to a newer version - preferably the latest one, but at the very least Firefox 3.6 instead. The move - which will be the first time it has undertaken such a step - could potentially bring an additional 12 million users into the Firefox 4 fold.

Several weeks ago Mozilla released the last security patch for Firefox 3.5 as the release approaches its end of life.

The software made its debut back in 2009.

It will be interesting to see reactions to Mozilla’s new automatic

upgrade plan, not to mention the overall effect on Firefox 4 usage.

In the meantime, there seems to be no end of good news about the winning open source browser, including the new IonMonkey just-in-time (JIT) compiler as well as speed improvements for those using Firefox on Linux. Firefox 4 also recently announced that it had surpassed 100 million downloads in its first month.

Will Firefox 4 win this round of the browser wars? Only time will tell. As of today, though, things are looking pretty good.

Appeals Court Won’t Reconsider Facebook Settlement

A federal appeals court has refused to reconsider its decision ordering two former Harvard classmates of Facebook founder Mark Zuckerberg to accept a multimillion dollar settlement over the company.

Twins Cameron and Tyler Winklevoss sued Zuckerberg, saying he stole the idea for the social networking site. Both parties reached a settlement in 2008, but the Winklevosses claim they were misled during settlement talks.

Last month, a three-judge panel of the 9th U.S. Circuit Court of Appeals upheld the settlement, which calls for a $20 million cash payment and stock in the company now valued in the tens of billions.

On Monday, the court declined to assign the case to a special 11-judge panel for reconsideration.

The Winklevosses still could appeal to the U.S. Supreme Court.

Tyler Winklevoss declined comment Monday.

Cyber-Crooks Eye Apple Macs with Fake Anti-Malware

The days when Mac users need not worry about their computers getting infected with malicious software may be coming to an end.

Internet security experts say that cyber-criminals have begun targeting users of the increasingly popular computers from Apple Inc with one of the most pernicious types of malware: fake anti-virus programs.

To date, hackers have focused on writing malicious software for machines running Microsoft Corp’s Windows operating system, which inhabits more than nine of every 10 PCs.

But Macs grow in number, they are becoming more attractive targets.

"Only once a platform has a certain level of market share does it become profitable for malware to attack it," said Dino Dai Zovi, co-author of The Mac Hacker’s Handbook. "As the Mac becomes more popular there will be more and more threats."

Security firm McAfee has seen "a steady stream" of these anti-malware

viruses appear over the Internet in the past week as it scours the Web for malicious software, said Dave Marcus, one of the company's top researchers.

The fake anti-virus malware is downloaded when people click on links from tainted search engine results for popular queries, Marcus said. It also spreads when users click on links to malicious sites that might be included in emails, Tweets or Facebook messages.

A spokesman for Apple declined comment.

Enforcing cybersecurity is becoming increasingly difficult with the proliferation in recent years of interconnected devices. The hacking of Sony's PlayStation Network - which unearthed data on more than 100 million users in the largest single Internet hacking scheme ever - underscored how exposed consumers can be.

Malware ranges from software that runs in the background to break into private data, to programs such as fake anti-virus software intended to help hackers profit.

These programs cause messages to pop up saying a machine has been infected with a virus. They offer to sell a fake anti-virus software package to clean up the problem. If the user pays the $80 to $100 for the software, the messages generally disappear.

But if the user fails to pony up, the annoying messages persist.

"This is the first time we've seen something hit en masse," said Chet Wisniewski, senior security adviser with anti-virus software maker Sophos, a rival of McAfee.

Wisniewski's company located a version of the fake anti-virus software for Macs that caused pornography to show up on a machine's screen every few minutes, to convince users their machines did indeed need to be cleaned of malware.

Sophos is one of a handful of security firms that sell anti-virus software for Macs. Others include McAfee and Symantec Corp. Apple already includes basic anti-virus software as part of its Mac OS X operating system.

Independent Mac security experts believe there is enough security built into the OS X operating system to protect users, given the current level of risk.

If users want extra protection, they should obtain anti-virus software from a company that they are sure is a legitimate vendor, said Dino Dai Zovi, co-author of The Mac Hacker's Handbook. He advised users to obtain that software through the Mac App Store.

One day, he said, it will become necessary to purchase special protection for Macs, but that time has not yet arrived.

New Virus Scam Attacks Macs

A frequent debate topic between Mac and Windows fans is Apple's

susceptibility to viruses and other malware. Some say Mac is an intrinsically safer platform and Macs are not nearly as virus-prone as PCs and other devices using Windows. Others contend that, with their smaller market share, Macs are simply not a target worth hacking.

Now, a new fake anti-virus software is making more Mac owners virus-aware. According to news reports, AppleCare has indicated that calls related to this malicious app - called MAC Defender, MacSecurity, or Mac Protector - are up dramatically.

A memo that has surfaced on the Web, reportedly an internal communication to Apple support staff, instructs how to handle such calls.

Key points in the memo include "do not confirm or deny that any such software has been installed," "do not attempt to remove or uninstall any malware software," and do not escalate or send the customer to the Apple Retail Store.

According to Mac security firm Intego, MAC Defender targets users of that platform primarily through "SEO poisoning attacks," in which Web sites with malicious code use search optimization tricks to rank at the top of search results. A user who clicks on that search result is sent to a Web site that shows a fake screen and a fake malware scan, after which it tells the user that the computer is infected.

Javascript on the page automatically downloads a compressed ZIP archive file. If the "open ’safe’ after downloading" option in Safari is enabled, the file is them unzipped and the user is presented with a Setup Installer.

If the user proceeds with installation, MAC Defender launches. Intego describes the application as "very well designed," with a professional look, a number of different screens, attractive buttons, and correct spelling.

Once installed, MAC Defender indicates that the computer is infected, and then opens Web pages for pornographic sites every few minutes. To counter the "virus," the user is prompted to buy into MAC Defender’s "anti-virus" protection service.

After a credit card number has been entered into a license purchasing page, the Web porn and virus warnings stop. But there is no service, and the user has just given the malware authors a credit card number.

Intego recommends not installing the application to begin with, of course, and to uncheck the "open ’safe’ files" option in Safari or other browsers.

This kind of fake anti-virus software has, for years, been the bane of many Windows users’ existence, but this is the first time it’s been designed for Mac. In fact, reports indicate that early versions of the malware still showed a Windows interface.

Although a rare example, MAC Defender/MacSecurity/Mac Protector is likely to be followed by an upsurge of such attacks. Macs now have an installed base big enough to be worthy of attention by hackers, and security experts have noted that a new Mac-oriented, point-and-click malware building kit is on sale in the criminal underground.

The Top 20 Strongholds for Desktop Linux

As a server OS, Linux has long been highly successful and a poster child for open source. For example, Linux currently powers a majority of the world s web servers and supercomputers. As a desktop OS, however, Linux has yet to gain mainstream acceptance.

That said, there are some countries where people have embraced Linux on the desktop to a greater degree than most.

Since you probably wouldn t be able to guess which these countries are no matter how hard you tried, we have highlighted them in this article.

Top 20 countries by Linux market share

We looked at desktop OS market share, in this case defined as the share of computers used to access the Web. It s basically the only metric out there that can give us an estimate of actual market share of actively used computers. The numbers are based on aggregated visitor stats for more than three million websites, courtesy of Statcounter.

As we collected the data for this article, we couldn t help but make a few additional observations that you might find interesting.

- Linux is most definitely a niche OS on the desktop: In most countries, Linux has less than 1% market share.
- The Linux vs. Windows situation: In no country is Linux anywhere near replacing Windows on the desktop, but this shouldn t come as a surprise.
- The absence of the US and UK: The United States is far outside the top 20, with a 0.73% desktop OS market share for Linux. This by the way happens to be the exact same market share as Linux has in the United Kingdom.
- The top countries in Europe are, in order: Macedonia, Finland, Spain, Czech Republic, France, Italy, Estonia and Germany.

Sweden, where we are based, sadly didn t make this list. We just managed a measly 1.09% desktop OS market share for Linux, but at least that s above average.

If you are wondering what Linux s desktop OS market share is in the various world regions, here are the numbers:

- Worldwide, 0.76%
- Europe, 1.14%
- South America, 0.88%
- North America, 0.72%
- Oceania, 0.72%
- Africa, 0.45%
- Asia, 0.34%

In other words, Europe comes out as the overall most Linux-friendly world region.

Why these ’low’ numbers are not bad at all

Linux may currently be a niche desktop OS, but that doesn t necessarily have to be a bad thing. It s often described as the ’tinkerer s OS,’ and it s hard to see how it could go mainstream and retain that quality. If

you keep that in mind, it s quite possible that Linux will never go mainstream on the desktop, but will continue to flourish in a similar way it is now, with a relatively small but very dedicated community of users.

And when we say ’relatively small’ we really mean relatively. The worldwide Linux desktop OS market share (0.76%) coupled with the number of Internet users (1.97 billion) indicates that there are at least 15 million active desktop Linux users out there.

We say ’at least,’ because that number is probably significantly higher since there is a lot of overlap in these stats with people who use more than one OS and more than one computer.

That s not a small community by anyone s standards (except maybe Facebook s ;)).

Notes about the data: The numbers are for the three-month period of February through April 2011 and are taken from StatCounter Global Stats. StatCounter bases those numbers on aggregated visitor stats for more than three million websites. To avoid statistical anomalies caused by small samples, we didn t include any countries with fewer than 250,000 Internet users.

The ’Post-PC’ Era Is Here - But Don’t Junk Your PC Just Yet

Has the much-discussed "post-PC era" finally begun? The term has been tossed about for years by industry executives and pundits alike. Its most recent high-profile use came during Steve Jobs’ iPad 2 unveiling in March, when the Apple CEO/guru called the iPhone, iPod, and iPad "post-PC devices" that needed to be more intuitive and easier to use than conventional desktops or laptops.

Well, add Forrester Research to the list of industry watchers who believe the post-PC era has begun. In a new report released Tuesday, Forrester analyst Sarah Rotman Epps says that computing devices - and how we interact with them - are currently undergoing a dramatic shift to:

* Ubiquitous computing: Mobile devices with sensors such as accelerometers, gyroscopes, and geolocators are freeing us from the stationary limitations of desktop PCs.

* "Casual" computing: Instant-on/always-on smartphones and tablets remove the formal boot up/shutdown process of the desktop.

* A more intimate experience: Tablets and smartphones are kept close to your body, whereas using a laptop or desktop is "arms-length activity," writes Epps in a blog post.

This means that consumers are using computing devices in intimate places, including the bedroom. Sounds like a boon to couples’ therapists to me.

* Physical interaction with devices: Touchscreens, voice input, motion-sensing devices such as Microsoft Kinect, and cameras with facial recognition allow your "body and voice" to control the machine. By comparison, the desktop’s mouse/keyboard interface is more abstract and less personal.

What’s it all mean? Certainly, the mobility and ubiquity of today’s tech devices is changing the way interact with our digital assistants. But the laptop and desktop aren’t going away anytime soon.

"So what does ’post-PC’ mean, anyway? It doesn’t mean that the PC is dead," Epps writes. In fact, Forrester forecasts that U.S. consumer laptop sales will grow at a compound annual growth rate of 8 percent between 2010 and 2015, and desktop sales will decline only slightly.

And while 82 million American consumers will own a tablet in 2015, more than 140 million will own a laptop, Forrester predicts.

"In the post-PC era, the ’PC’ is alive and well, but it morphs to support computing experiences that are increasingly ubiquitous, casual, intimate, and physical," says Epps.

Could The Internet Spell The End of Snow Days?

Could the Internet mean the end of snow days? Some schools think so, and they are experimenting with ways for students to do lessons online during bad weather, potentially allowing classes to go on during even the worst blizzard.

"Virtual snow days" would help ease pressure on school calendars. Because districts are required to be in session for a certain number of hours or days, losing teaching time to winter weather can mean extending the school day or cutting short spring break or summer vacation.

And canceling school in the winter, when some of the most difficult material of the year is covered, risks leaving students with a learning deficit heading into the spring, when many states administer standardized tests.

"Even if you can’t continue on at the same pace, being able to keep students on track can make a huge difference," said Doug Levin, executive director of the nonprofit State Educational Technology Directors Association.

Virtual learning, which has been widely used by colleges and universities for years, is becoming more viable for younger students as teachers and administrators grow comfortable with the technology. Online learning also saves money because districts don’t have to pay for transportation, electricity and custodians.

But there are obstacles, too. Many families don’t have Internet access with speeds that would support complex classroom-style work, especially in rural areas and impoverished inner cities. Families with multiple children - without multiple computers - could be hard-pressed to keep up.

And some people say kids just need an occasional extra day off in the depths of winter.

"When deep snow falls, the world becomes quiet and still. And if we listen to our instincts, we settle in and enjoy the pure joy of not doing," David Santner wrote on the website for the Poughkeepsie Day School in New York, where his son is a middle schooler, after the school

turned to online learning during a spate of winter storms.

For schoolchildren, old-fashioned snow days used to mean languorous hours spent playing outside in the drifts, watching television or sipping hot chocolate. But someday, kids who can’t get to the classroom might just sit down with their computers.

Josie Holford, head of the Poughkeepsie school, which had six snow days and four late starts this past winter, said it’s possible to enjoy the outdoors and keep learning. Students in one class were told to draw a picture in the snow for a lesson on angles and to take a picture of their creation.

"We have to recognize as teachers, educators, all of us, that we are in a completely different landscape, and that learning really isn’t confined to a textbook or a teacher anymore," Holford said. "We all have to be learning all the time. Why should a snow day stop the progress of learning?"

At St. Therese School in the Kansas City suburb of Parkville, students recently did a virtual make-up day after classes were canceled six times because of weather.

As she used a computer drawing program to complete an art lesson in her kitchen, seventh-grader Cameron Mottet predicted her classmates would embrace the system, especially if it means "they don’t have to go to school in June."

Cameron’s older sister, whose school isn’t making up days virtually, has grumbled that she will be in class while Cameron is free to hang out at the pool.

The first experiments with virtual snow days began a few years ago as individual teachers started logging on during poor weather to drill older students. Since then, entire schools and districts have joined in, using websites such as Skype and YouTube to keep students as young as kindergarten studying during storms.

An increasing number of teachers have their own websites, so sometimes starting virtual lessons is as simple as telling parents to check on snow days to see if any assignments are posted. Other times, the makeup work occurs afterward, with students completing assignments from home on days set aside for teacher training. Students can chat online with their teachers and ask questions via email.

In one school, younger students were directed to a website to play online money games, while older students in another school completed a simulation program to test how the angle of a baseball pitch affects the distance a ball is thrown.

The experiments appear to be the most prevalent in affluent private schools like Cameron’s, where only three of 643 students lacked a home computer.

At an all-girls boarding school in Simsbury, Conn., some teachers started using the Internet for lessons when roads become impassable so students who commute didn’t fall behind the others who live on campus.

"It’s been a really bad winter, so the teachers were grateful they could use these tools and not lose a day or cram too much material in one

day," said Vivian K. Elba, director of marketing and communications at Ethel Walker School.

But the efforts aren't limited to wealthy, private schools. The Mississinawa Valley district on the Indiana-Ohio state line has led Ohio's push for virtual snow days. Fifty-two percent of the district's 700 students qualify for free or reduced-price lunches.

Since Mississinawa got permission last fall to make up two snow days electronically, four other Ohio districts joined the pilot program. Superintendent Lisa Wendel has received calls from other states interested in virtual make-up days.

"It is going to continue to snowball in this country," said Wendel, whose district has been forced to call off classes 11 times this school year.

However, Wendel questions whether virtual snow days will continue in her own district. Ohio lawmakers have thrown out a provision allowing the practice, citing concerns that poor students without home computers and rural students without Internet access could be at a disadvantage. Lawmakers continue to debate the issue.

Jalisa Rush, a seventh-grader in the district who has her own laptop, said she and her friends spent their e-days chatting on Facebook as they did online assignments that included calculating the calories and transfats in favorite foods. Because some of the projects were more creative, she didn't mind committing five to six hours to them.

"I thought it was really exciting and something new to try, which was really pretty great," she said. But she added: "It gets a little harder because you didn't really have the teacher there to explain something if you have a question."

Carol Hussin, principal of Cameron's St. Therese School, said some parents have complained the online work took longer than the six hours teachers intended, but others said they enjoyed getting a glimpse of their children's studies.

"I think it's a great tool to have," said Cameron's mother, Jane. "Obviously it's not going to replace going to school. But for situations like this, I think it's wonderful."

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or

internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.